ATTACHMENT A

REMARKS

Considering the matters raised in the Office Action in the same order as raised, headings have been provided, as appropriate, throughout the specification.

The disclosure has been objected to because the phrase "a priori" appearing at page 3, line 31 and page 7, line 35 has been underlined. It is respectfully submitted that the underlining of this phrase is appropriate. The phrase "a priori" is a Latin phrase and the standard rules of grammar provide for underlining thereof.

Claims 1-9 have been rejected under 35 USC 102(e) as being "anticipated by" the Veil et al patent ("Veil"). This rejection is respectfully traversed.

The Veil patent discloses a method and system for secure transactions in a computer system. The Veil system comprises a computer 114 and a security co-processor 122 which are arranged so that the secure computing environment 104 is separate from the traditional computer environment 102 (see column 7, lines 8-16 and Figure 4). An interface 134 located between the two computing environments 102 and 104 acts as a firewall (see column 9, lines 1-2 and Figure 4).

The purpose of the above-described architecture in the Veil reference is to enable electronic transaction applications, such as credit purchases, to be "executed in a secure computing environment outside of the reach of computer hackers" (see column 6, lines 50-54). This purpose is achieved by distributing the processing of the electronic transaction so that the security co-processor 122 is responsible for processing sensitive data whereas the computer 114 only processes non-sensitive data (see column 7, lines 29-36). For example, the security co-processor 122 encrypts the sensitive data or wraps this data in cryptographically signed messages before transfer thereof to the computer 114 for completion of the transaction (see column 7, lines 37-46). Thus, in the system of the Veil patent, "the sensitive data is never processed by the computer 114 in the traditional computing environment 102 and it is therefor not susceptible to attack." (See column 7, lines 45-49.)

Although there is some resemblance between the architecture of Veil and that of the present invention wherein a processor and a peripheral perform different functions, it is respectfully submitted that there are important differences and that claim 1 patentably defines over the Veil reference. In this regard, the peripheral of the present invention performs

verification operations so as to check that the processor is operating properly. More particularly, as recited in claim 1, the peripheral "computes a code for each elementary operation performed by the processor and verifies proper operation of all or part of the executed program." It is respectfully submitted that such codes differ from, and should not be confused with, cryptographic data. (In this regard, it is clear from the specification that the data processed by the present invention could be transmitted outside of the system in a non-encrypted form). The purpose of computing of a code for each elementary operation performed by the processor and verifying proper operation of all or part of the computer program is not to protect the data against hackers, but, instead, to check the properties of the data and to derive therefrom whether the processor is operating correctly. It is also noted that the peripheral computes code for any and all types of data received from the processor and not only for sensitive data.

Although the present invention is obviously not limited to the particular examples set forth in the specification, an example of such coding is set forth at page 2, lines 32-34. In this example, multiplication by a prime number A is provided and computational errors can be detected by detecting the loss of divisibility by A. This property conservation can be used to help in detecting operating faults of the system (see page 1, lines 1-5). Another example is set forth at page 5, lines 8-19.

It is respectfully submitted that the security co-processor of Veil does not compute codes within the meaning of that word as claimed in the claims but rather merely encrypts sensitive data, and, moreover, clearly does not verify the proper operation of the executed program. The security co-processor of the Veil patent is not concerned with error detection with respect to system behavior, and, as indicated above, does not receive "at least the input data codes, the operands, and the nature of the operation for each elementary operation performed by the main processor," and does not compute "a code for each elementary operation performed by the processor" and verify "proper operation of all or part of the executed program." Thus, for at least these reasons, it is respectfully submitted that claim 1 patentably defines over the Veil patent.

With respect to claims 2-9, these claims are patentable for at least the reasons set forth above in support of the patentability of claim 1.

Allowance of the application in its present form is respectfully solicited.

END REMARKS